UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v.

JOHN STUART,

Defendant.

21-CR-007

NOTICE OF MOTION

MOTION BY:	Jeffrey T. Bagley, Assistant Federal Public Defender
DATE, TIME & PLACE:	Before the Honorable Jeremiah J. McCarthy, United States Magistrate Judge, Robert H. Jackson United States Courthouse, 2 Niagara Square, Buffalo, New York, **on the papers submitted.**
SUPPORTING PAPERS:	Memorandum in Support of Motion to Compel by Assistant Federal Public Defender Jeffrey T. Bagley, dated July 8, 2022
RELIEF REQUESTED:	Motion to Compel Discovery
DATED:	Buffalo, New York, July 8, 2022

/s/ Jeffrey T. Bagley
Jeffrey T. Bagley
Assistant Federal Public Defender
Federal Public Defender's Office
300 Pearl Street, Suite 200
Buffalo, New York 14202
(716) 551-3341, (716) 551-3346 (Fax)
jeffrey_bagley@fd.org
Counsel for Defendant John Stuart

TO: Laura A. Higgins
Assistant United States Attorney
Western District of New York
138 Delaware Avenue, Federal Centre
Buffalo, New York 14202

UNITED STATES DISTRICT FOR THE
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v.

JOHN STUART,

Defendant.

MEMORANDUM IN SUPPORT OF MOTION TO COMPEL

No. 21-CR-007

INTRODUCTION

Mr. Stuart previously moved for suppression of evidence seized as a result of a search warrant for the premises at 1010 Cleveland Drive in Cheektowaga, New York, arguing that the information in the warrant purporting to support probable cause was weak and stale. This Court recommended that the motion be denied and Judge Lawrence J. Vilardo adopted that recommendation.

Since that time, however, the defense has since learned that the scope of the FBI's investigation was much broader than it has let on – even, apparently, to its own prosecuting attorney. In his application in the support of the search warrant, FBI Special Agent Michael Hockwater claimed to be relaying information from an undisclosed foreign law enforcement agency ("FLA") that an IP address, later learned to be associated with the Cleveland Drive address, had accessed a child pornography website on May 28, 2019. But the defense has learned that this case is merely a small part of a vast multi-district, multi-national pornography investigation. Other exceptionally similar, if not identical, cases have sprung up throughout the county, and the defense's investigation into those cases have revealed that the government's disclosures to date have been inadequate.

At status conferences in April and May of 2022, this information was relayed to Judge Vilardo, who at that time had assumed his duties on the case as the District Judge. Based on the newly discovered information and representations made by counsel about the nature of that information, the defense requested leave to file a motion to compel. Judge Vilardo granted that motion and referred the matter to this Court for disposition.

Accordingly, Mr. Stuart now moves under *Brady v. Maryland*, and Rules 12(b)(3)(E), 16(a)(1)(E) and 16(a)(1)(F) of the Federal Rules of Criminal Procedure for an order compelling further discovery.

THE SEARCH WARRANT

Hockwater's application indicates that the FBI was told by a foreign law enforcement agency that a certain IP address has accessed a certain website:

> In August 2019, a foreign law enforcement agency (referenced herein as "FLA") known to the FBI and with a history of providing reliable, accurate information in the past, notified the FBI that FLA determined that on May 28, 2019, IP address 74.77.4.235 "was used to access online child sexual abuse and exploitation material" via a website that the FLA named and described as the TARGET WEBSITE.
>
> FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigative information with FLA and FLA sharing criminal investigative information with U.S. law enforcement, across disciplines and including the investigation of crimes against children. FLA advised U.S. law enforcement that it obtained that information through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws. FLA further advised U.S. law enforcement that FLA had not interfered with, accessed, searched or seized any data from any computer in the United States in order to obtain that IP address information. U.S. law enforcement personnel did not participate in the investigative work through which FLA identified the IP address information provided by FLA.

We have come to learn that was a batch warrant. That is, warrants nearly identical to this one, with only the name of the suspect and other individualized information changed, were

issued by the FBI throughout the country. (*See* Case Comparison, attached as Ex. A.) Agent Hockwater just filled in the blanks – name, home address, IP address, etc. The boilerplate warrant, we believe, was actually drafted by other FBI agents, likely in Massachusetts. Each of these warrants follow a strikingly similar pattern: the FBI claims to have learned from a FLA tip in August of 2019 that a certain IP address accessed a target website in April or May of 2019.

Also common to all the warrants is the omission that this information was only learned after a much broader, far-reaching investigation, involving several countries and going back years. Indeed, an FBI document demonstrates that the FBI opened its preliminary investigation in this matter in January 2017, more than two years before the IP addresses that had purportedly visited the target websites were identified by a foreign law enforcement agency and transmitted to the FBI. (*See* Exhibit B.) In an affidavit that arose from the same operation as this case, law enforcement described the investigation as "collaborative" between U.S. and foreign law enforcement. *United States v. Thomas S. Clark*, Case No. 2:21-MJ-00147-JLW (W.D. Wash., March 11, 2021) (Complaint) ("Clark Complaint") attached as Ex. C, at ¶ 5. Press releases and the volume of information that the FBI obtained in reference to this investigation are additional evidence that this was a joint operation, where U.S. law enforcement were working hand in hand with foreign law enforcement agencies to share information, take over targeted websites, and identify visitors to target websites.

At least in other cases, however, the government has disclosed some information about the investigation, including the following:

- The identity of the FLA that provided the tip.
- The name of the website.

- The tip itself.
- Documents related to the tip.
- That the website's server was located in a third country.
- The identity of that country.
- That the website's server was seized and run by an FLA.
- That it was that third country's law enforcement agency that actually seized the server.
- That it was only after this third country seized the server and covertly ran it, that IP addresses were identified.

None of this information was provided to the defense in this case. (Nor, does it appear, that any of this information was relayed to the magistrate judge before he issued the search warrant). In fact, none of this information was even provided to the Assistant United States Attorney prosecuting this case, who has indicated in court that she was unaware of any of the above. This is troubling because each "prosecutor has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case, including the police." *Kyles v. Whitley*, 514 U.S. 419, 438 (1995). How can the government claim to have complied with its *Brady* and disclosure obligations when it does not even know how the tip was generated, or what foreign law enforcement agencies are involved? Or that the investigation dates back years and involves multiple countries? It can not.

It would be one (still problematic) thing for the prosecution to have reviewed all the above information and made an affirmative choice not to disclose any of it. It is far more troubling for the United States Attorney's Office to have so little knowledge about its own agents' investigation – an investigation that that lead to the issuance of warrant to ransack a man's home, and serious criminal charges.

The number of similar cases using similar, if not identical, language to the search warrant affidavit indicates a large-scale, coordinated investigation into websites hosted on the Tor network akin to the Playpen investigation.[1]

LEGAL STANDARDS

Federal Rule of Criminal Procedure 16(a)(1)(E) requires the government, upon request, to turn over any item in its possession, custody, or control if the item is material to preparing the defense; the government intends to use the item in its case-in-chief at trial; or the item was obtained from or belongs to the defendant.

Evidence is material within the meaning of Rule 16 "if it could be used to counter the government's case or to bolster a defense...." *United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir. 1993). "To obtain discovery under Rule 16, a defendant must make a prima facie showing of materiality." *United States v. Clarke*, 979 F.3d 82, 97 (2d Cir. 2020). While "[m]ateriality means

---

[1] In December 2014, the FBI received a tip from an FLA that a Tor web site called "Playpen" was hosting child pornography, its actual IP address was publicly visible and appeared to be located within the United States. After some additional investigation, the FBI in early 2015 obtained a search warrant and seized the server hosting the site.

But instead of shutting Playpen down, the FBI continued to operate this child porn site for nearly two weeks. While the FBI was operating the site, it secured a single warrant to send malware to thousands of unsuspecting visitors of the site nationwide, exploiting a vulnerability in the Tor browser to install malware on their computers.

The FBI's malware, described by it as a Network Investigation Technique ("NIT"), searched for and copied certain identifying information from users' computers and sent that information outside of the Tor network back to the FBI in Alexandria, Virginia. Once the FBI obtained an IP address from the NIT's transmissions, it served subpoenas on Internet service providers to learn the names and addresses associated with that IP address. The FBI then obtained warrants to search and seize evidence associated with child pornography at those locations. The common denominator in these warrants nationwide were the supporting affidavits, which had nearly identical information.

This massive sting and hacking operation has been described as the most extensive use of government malware by a U.S. law enforcement agency in a domestic criminal investigation. Hundreds were prosecuted across the country and more than a thousand computers around the world were infected by its malware.

more than that the evidence in question bears some abstract logical relationship to the issues in the case," *Maniktala*, 934 F.2d at 28 (quoting *United States v. Ross*, 511 F.2d 757, 762-63 (5th Cir. 1975)), the "materiality standard [of Rule 16] normally is not a heavy burden; rather, evidence is material as long as there is a strong indication that it will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." *United States v. Stein*, 488 F. Supp. 2d 350, 356-57 (S.D.N.Y. 2007) (citation omitted).

The government has the duty to disclose *Brady* information even without a request by the defense. *United States v. Agurs*, 427 U.S. 97 (1976). The information includes not just evidence that affirmatively exculpates a defendant, but also may include information that impeaches the credibility of Government witnesses. *See United States v. Bagley*, 473 U.S. 667, 676–77 (1985). Indeed, the extent of the disclosure required by *Brady* is "dependent on the anticipated remedy for violation of the obligation to disclose: the prosecutor must disclose evidence if, without such disclosure, a reasonable probability will exist that the outcome of a trial in which the evidence had been disclosed would have been different." *United States v. Coppa*, 267 F.3d 132, 142 (2d Cir. 2001). "Like the extent of the required disclosure, the timing of a disclosure required by *Brady* is also dependent upon the anticipated remedy for a violation of the obligation to disclose." *Id.*

ARGUMENT

To properly litigate the pertinent Fourth Amendment issues before the Court, including addressing matters of reliability and veracity, important factors under *Gates* in considering the totality of the circumstances, the defendant needs more discovery.

Particularly in light of the new information from other District Court prosecutions, the defense must be provided at least as much information as was provided there, including (1) the

name of the FLA country, (2) the identity of the foreign country that actually infiltrated the website, (3) the identity of the country that actually deployed the technique that initially identified the defendant's IP address, (4) the tip itself; (5) how was this information gathered, beyond what the government has vaguely coined a "independent investigation."

The materials available suggest that there was, at minimum, a collaboration between the United States and the FLAs in the investigation in this case. *See United States v. Clark*, *supra*. Mr. Stuart is entitled to discovery that further reveals the level of collaboration between the United States and the FLAs because it goes to the heart of whether the FLAs' investigations involved searches within U.S. territory, and whether the FLAs acted with U.S. agents, at the behest of U.S. agents, or as agents for their American counterparts, such that there was a "joint venture" or that it constituted activities which would shock the conscience in violation of the Fourth Amendment.

An expert declaration submitted in a case virtually identical to Mr. Stuart's suggests that the specific IP address could not have been identified without running a NIT – an NIT just like the malware developed by the FBI – or, in the alternative, an error-prone traffic analysis technique. *See* Declaration of Steven Murdoch at ¶ 22-32, *United States v. Sanders*, No. 20-cr-00143 (E.D. Va. Sept. 17, 2021), ECF No. 464-2, attached as Exhibit D. Either scenario would significantly undermine the veracity of the affidavit and its probable cause showing. The deployment of a NIT would constitute an unlawful warrantless search, the results of which could not be considered in Agent Moynihan's affidavit. *See United States v. Tagg*, 886 F.3d 579, 584 (6th Cir. 2018). The use of a NIT would also reveal a substantial misrepresentation in the affidavit, which relies on Hockwater's assurance that no computer in the United States had been searched. "Malware" is short for "malicious software" which is designed to gain access to or damage a computer without the owner's consent. Malware includes spyware, viruses, and any

type of malicious code that infiltrates a computer. In the *Playpen* investigation, for instance, the malware used by the government was surreptitiously disseminated through a Tor hidden service, designed to pierce the anonymity provided by Tor. Thousands of computers, located all over the world, were searched during the *Playpen* investigation in this way.

Alternatively, the fact that the traffic analysis technique described in Professor Murdoch's declaration is inherently error-prone would undermine the strength and reliability of the tip such that no magistrate, had he or she been aware that this technique was used to obtain the IP address, would find there was probable cause. *See* Exhibit D at ¶ 22-32.

Importantly, The technique used to identify the IP address is also material to whether, and to what extent, U.S. law enforcement directed, assisted, and/or participated in the investigation. In the affidavit, Hockwater claimed that U.S. law enforcement had not participated in the investigative work "through which FLA identified the IP address information provided by FLA." However, this deliberately obscures the fact that there were two distinct FLAs from two different countries involved in obtaining the IP address. The Agent's assurances that U.S. law enforcement did not "participate" only applied to the tip-giving FLA, not to the as-yet unnamed FLA who the FBI may have worked closely with, or shared malware with. Indeed, the government has made *no assurances* as to the unnamed FLA.

Accordingly, Mr. Stuart has made a sufficient showing, to the extent possible with the materials available to him, that this information is material to preparing his defense, and it is exculpatory under Fed. R. Crim. P. 16(a)(1)(E) and *Brady*. Moreover, because the anticipated remedy is a *Franks* hearing and suppression of evidence obtained as a result of a misleading warrant, this information must be turned over now (it should have been turned over already). *See Coppa*, 267 F.3d at 142 ("[T]he timing of a disclosure required by *Brady* is also dependent upon the anticipated remedy."). Indeed, all discovery was supposed to be completed by February 26,

2021 (*see* Scheduling Order, Docket No. 14) and the defense had made Rule 16 demands, including the name of the FLA, in its omnibus motion filed October of 2021. (Docket No. 27).

WHEREFORE, Mr. Stuart makes this motion to compel the following, but not limited to:

1. The identity of the FLA that issued the tip or information.
2. The identity of the FLA that seized the computer server hosting the target website.
3. The author of the FLA notification.
4. The identity of the U.S. law enforcement agency that received the notification.
5. The complete content of the notification, including information or tactics and techniques used by the FLA to determine the identity of the IP addresses accessing the website, and any documentation/memorandum/agreement regarding the investigative technique used.
6. The number of tips provided to the United States by the FLA as part of this vast investigation.
7. The number of IP addresses identified as part of the investigation.
8. Any record of action taken in response by the United States to the FLA notification.
9. Any documentation/memorandum/agreement regarding collaboration between the United States and *all* FLAs involved in the investigation.
10. All cover sheets correspondence or other documentation documenting the totality of the tip/information provided by the FLA.

Dated: Buffalo, New York
July 8, 2022

Respectfully submitted,

/s/ Jeffrey T. Bagley
Jeffrey T. Bagley
jeffrey_bagley@fd.org

/s/ Timothy P. Murphy
Timothy P. Murphy
timothy_murphy@fd.org

Assistant Federal Public Defenders
Federal Public Defender's Office
300 Pearl Street, Suite 200
Buffalo, New York 14202
(716) 551-3341

Counsel for Defendant